COMPUTER USE POLICY & AGREEMENT

1. PURPOSE

The purpose of this policy is to specify the appropriate use of computers, computer equipment, software, systems, networks, files, electronic mail, and the Internet by employees of the *Agency*. This policy applies to full or part-time State employees; volunteers and interns authorized to use State computing resources; and contractors, vendors or individuals associated with the State and authorized to use State computing resources, hereinafter referred to as 'Authorized Users.'

2. POLICY

Review and Signature by each Authorized User is required annually.

3. DEFINITIONS

3.1. "Computer use" means the use of a State computer and/or the State's electronic systems, including networks, software, electronic mail (e-mail) use of the Internet, and storage of and access to files through such computers or systems.

3.2. "Commissioner" means the Commissioner of the *Agency/Department/Commission*. *(Commissioner can be modified throughout the document to Executive Director or other as appropriate.)*

3.3. "*Agency Abbreviation*" or "the Agency or Department" means the *Agency/Department/Commission*. *(These references can be modified throughout the document to Department, Commission, or other as appropriate.)*

3.4. "DoIT" means the New Hampshire Department of Information Technology.

3.5. "Supervisory personnel" means the employee's immediate supervisor or a person at a higher supervisory level within the employee's chain of management within the Department.

4. BACKGROUND

Improper computer use may present significant problems for the Department and the State as a whole. Depending upon the circumstances, misuse might result in damage to the State's systems or equipment, might result in lost productivity or increased expense to the State or might be damaging in other ways. The use of the State's computer system to store personal files, music or videos, for example, utilizes storage space on the system, making that space unavailable for State business, while the use of the Internet for personal purposes utilizes limited bandwidth that is legitimately intended for conducting official activity. This policy has been adopted in order to address such concerns.

5. PRIVACY & BUSINESS USE

5.1. It is the policy of the Agency to grant computer use to Authorized Users in order to facilitate communication and perform their assigned job duties. Computers, computer equipment, files and e-mail are the property of the Agency. The Agency reserves the right to monitor, or request the monitoring of computer use for purposes including, but not limited to, checking system performance, ensuring that the system is used appropriately, and ascertaining bandwidth and storage capacity. Authorized Users should understand that they have no personal entitlement to privacy regarding their computer use. The Agency must also have access to an employee's computer files and e-mail if the Authorized User is not available.

5.2. Authorized Users do not have a personal privacy right in material created, received or sent via e-mail or the Internet, nor do they have a personal privacy right in information stored in computer files. Computer use is a privilege not a right. An employee's supervisory personnel, as well as others with appropriate authority, may curtail, limit, modify or eliminate that privilege at any time. Accepting computer use carries with it an expectation of responsible and acceptable use as defined by the State and its relevant agencies.

5.3. Computer use, as defined above, is limited to State business only. This means, for example, that State e-mail may not be used for purely personal activities, such as communications not related to State business; personal "blogging" or Internet use, or checking non-work personal e-mail accounts. During work periods which do not interfere with the completion of other job assignments, employees may, however, access any systems or websites which support Agency business functions (such as the NH FIRST Time Management System) or which are offered by or through the Agency to its employees.

5.4. All Authorized users who are granted computer use are expected to follow this policy. Improper computer use, including but not limited to failure to follow this policy, may result in the loss of some or all computer use privileges and may also result in disciplinary action as provided in the administrative rules of the Division of Personnel. Depending upon the circumstances, inappropriate computer use might also result in criminal prosecution under relevant state and federal laws, including but not limited to N.H. RSA 638: 16 – 19 (relating to computer crimes). In cases of misuse resulting in financial loss to the State, the employee might also be required to reimburse the State for damages, as well as any costs of collection and interest.

5.5. The Department may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was not subject to blocking software and report this immediately to your supervisor.

6. SPECIFIC POLICIES AND PROCEDURES

6.1. *Account Usage and Access*

6.1.1. Receiving an account is a privilege extended only to the Authorized User who signed for the account. Except as otherwise provided in this policy, no other person may use the account. Authorized Users must take reasonable precautions, including password maintenance and file protection measures, to prevent unauthorized use of their account. Authorized Users are required to change their passwords regularly.

6.1.2. Authorized Users may not share their personal access codes or passwords with others. If an Authorized User is unavailable for an extended period of time, access to their electronic data may be granted to their supervisory personnel upon request by the Agency Human Resources Administrator to the DoIT HR Administrator and the Director of Technical Support Services. In cases of extended unavailability, an employee may also, with the approval of his or her supervisory personnel, arrange to have his or her e-mail forwarded to specific individuals for the duration of the absence. In order to arrange for this option, the employee shall discuss with his or her supervisor the appropriate person to whom e-mails shall be forwarded. Following approval by the supervisor, the employee shall arrange for the forwarding of e-mail to the specified person for the specified period, if necessary contacting DoIT for assistance. The automatic forwarding/copying of state e-mail to an external destination is prohibited.

6.1.3. Authorized Users shall not store business files locally on computers unless authorized. If authorized, files must be routinely copied to network storage for proper backup.

6.1.4. It is a supervisor's responsibility to determine the positions in their respective divisions, bureaus, or units which should be granted computer use. It is also a supervisor's responsibility to, when necessary, arrange for the termination of such use by submitting a Help Desk request to DoIT.

6.1.5. At no time shall an Authorized User leave a computer without first ensuring that the computer is properly secured from unauthorized access.

6.1.6. Authorized Users shall move important information from e-mail message files to shared folders to ensure proper backup. Messages no longer needed shall be purged periodically.

6.1.7. Authorized users are responsible for all systems and information accessed by their assigned User ID.

6.1.8. Authorized users shall not 'remember' or cache logins and passwords.

6.1.9. Authorized Users shall not intercept, disclose or assist in intercepting or disclosing any electronic communications, except as authorized by this policy.

6.1.10. Providing false or misleading information for the purposes of computer use is prohibited under this policy.

6.2. ***Handling of Accounts on Cessation of Employment***

6.2.1. Access to an employee's account will be stopped upon cessation of an employee's employment unless permission is granted by the supervisor in charge of the bureau or equivalent unit, or that person's supervisory personnel, to allow continued access so as to enable the department, division, bureau or unit to access and retrieve necessary documents in the account. Once the required documents are retrieved, it is the supervisor's responsibility to notify their HR Administrator to arrange for termination of access to the account.

6.2.2. Supervisors of personnel whose employment with the Agency has ceased shall include as part of their exit checklist a specification of the steps which are to be taken in regard to the employee's electronic accounts and records.

6.3. ***Inappropriate Use of Systems***

6.3.1. A user will never make accessible or transmit any material that a reasonable person would construe as intimidating, harassing or offensive.

6.3.2. A user will not misuse or damage the State's computers, its systems or other users' information.

6.3.3. A user will not steal, abuse or damage resources, equipment or supplies belonging to the Agency.

6.3.4. Personal activities such as recreational game-playing, vacation planning, and product research on any State computer is prohibited.

6.3.5. Storing personal electronic files, including but not limited to documents, spreadsheets, pictures, videos, or music, on a State computer system is prohibited.

6.3.6. If a supervisor receives a complaint from any source regarding potentially inappropriate or unacceptable computer use by an employee under his or her supervision, or if he or she observes such potentially inappropriate use by an employee under his or her supervision, the supervisor shall advise the Agency Human Resources administrator of the potential unacceptable or inappropriate use. Depending upon the nature of the potentially inappropriate or unacceptable use, the Agency may deny or limit an employee's computer use. If an employee's supervisor concludes that the computer use in question is inappropriate or unacceptable under this policy, the supervisor may, in addition to the foregoing, initiate disciplinary action.

6.3.7. The Agency reserves the right to deny or limit an employee's computer use in order to stop any potential violation of this policy.

6.4. ***Examples of Acceptable Computer Use***

The following is a non-exhaustive list of **acceptable** computer use:

6.4.1. Communicating and exchanging information directly related to the business, mission or goals of Agency or the State of New Hampshire.

6.4.2. Publishing information relating to State business on the Internet with the approval of appropriate supervisory personnel.

6.4.3. With the approval of appropriate supervisory personnel, communicating or exchanging information related to professional development to maintain currency on topics of agency interest.

6.4.4. Applying for or administering grants or contracts for agency research or programs, as authorized by appropriate supervisory personnel.

6.4.5. Announcing new laws, rules, regulations, policies or procedures as authorized by appropriate supervisory personnel.

6.4.6. Use of the e-mail system by a collective bargaining unit for such business as is allowed under the terms of an applicable collective bargaining agreement. In such cases, the e-mail subject line must state that it relates to the business of the collective bargaining unit (for example, "SEA Business").

6.4.7. Accessing or using services found on the "Sunspot" State intranet site so as to access the State's employee benefit forms during the work day, so long as doing so does not interfere with the completion of other job assignments.

6.4.8. Accessing the NH FIRST Time Management System or the Administrative Services Online Pay Statement System (ASOPS) at times which do not interfere with the completion of other job assignments so as to review information or enter time or leave data.

6.5. ***Examples of Unacceptable Computer Use***

The following is a non-exhaustive list of **unacceptable** computer use. Employees shall not engage in computer use for these purposes or in these manners.

6.5.1. Communicating or exchanging information not directly related to the business, mission or goals of the Agency or the State of New Hampshire.

6.5.2. Browsing the Internet for non-business purposes regardless of access provided by agency filtering policies.

6.5.3. Publishing information on the Internet without the approval of the appropriate supervisory personnel.

6.5.4. Any purpose which violates federal or state law, or any computer use to access or distribute any illegal material, or for any illegal purpose.

6.5.5. Personal or private business, including but not limited to shopping, advertising or promotion.

6.5.6. Political lobbying.

6.5.7. Fund raising, public relations, or any similar activities which are not specifically related to agency activities or State government.

6.5.8. Accessing or distributing indecent or obscene materials.

6.5.9. Accessing or distributing computer games, jokes, chain letters, cartoons, sound files for amusement or entertainment purposes or accessing or distributing material not specifically related to State business.

6.5.10. Use in a manner that interrupts or disrupts network users, services, or equipment.

6.5.11. Intentionally seeking out information on, obtaining copies of, or modifying files and other data which is private, confidential or not open to public inspection, unless specifically authorized to do so by a person with appropriate authority.

6.5.12. Computer use to intentionally copy software, electronic files, programs or data which may be prohibited from such copying, unless a determination has been made by a person with appropriate authority that such copying is in fact permissible. Efforts to obtain such permission should be documented.

6.5.13. Intentionally seeking information on, obtaining copies of, or modifying files or data belonging to others without authorization of the file owner.

6.5.14. Seeking passwords of others or the exchange/sharing of passwords with others, including supervisors.

6.5.15. Intentionally representing oneself electronically as another person, unless specifically authorized to do so by that other person.

6.5.16. Intentionally developing programs designed to intimidate, offend or harass other users or to infiltrate a computer or computing system and/or damage or alter its software components.

6.5.17. Using profane or abusive language.

6.5.18. Harassment, including but not limited to sexual harassment, or creating or sending messages which might constitute intimidating, hostile or offensive materials on the basis

of age, gender, race, color, marital status, pregnancy, religion, national origin, sexual orientation, or physical or mental disability.

6.5.19. Any use that, in the determination of the Commissioner, reflects poorly on the agency or the State of New Hampshire.

6.6. ***Inappropriate Use of Software***

6.6.1. Only software owned by, licensed by, or freeware/shareware approved for use by the State can be installed on State equipment. State owned or licensed software may not be installed on personally owned equipment without the prior approval of supervisory personnel.

6.6.2. Software that has been licensed to the State must not be copied or moved to another site by the user. Users must exercise a high degree of care to protect software licenses from unauthorized access, misuse, theft, damage, destruction, or modification.

6.7. ***Ownership of Materials Developed on the Job***

All content developed on the job or while utilizing State facilities or resources, including licensed software, shall be the exclusive property of the State of New Hampshire.

6.8. ***Confidentiality and Nondisclosure***

State of NH information shall be classified as "Confidential' unless otherwise specified and shall be protected from unauthorized disclosure. Under no circumstances shall an authorized user disclose to the public, or to any other individual, any confidential information pertaining to the offices or departments serviced.

Storage of confidential information on mobile devices must be authorized by each agency per the Mobile Device Security Policy. Mobile devices known or believed to store confidential information must have the standard encryption product installed to protect information in the event the device is misplaced or stolen. Any loss of such device must be reported immediately to the employee's supervisor.

6.9. ***Department of Information Technology Statewide Standards and Policies***

DoIT periodically issues standards and policies which are applicable statewide and with which all State employees should be familiar. DoIT statewide standards and policies are located on the DoIT Agency Intranet at:

http://www.nh.gov/doit/intranet/toolbox/standards/index.php

6.10. ***Modified and Supplemental Requirements***

The Agency Commissioner may modify or amend this policy at any time and additional or supplemental requirements or limitations may be imposed within particular divisions, units, bureaus and offices of the Department. The Agency Commissioner may, if he or she concludes that to do so is appropriate in the circumstances, grant exemptions or waivers from, or modifications to, specific provisions of this policy as it applies to particular situations.

6.11. ***Failure to Abide by Policy***

Employees who do not comply with this policy, as from time to time amended, or who decline to execute the preprinted Employee Acknowledgement when requested to do so by their supervisor, may be subject to disciplinary action as described in the Administrative Rules of the Division of Personnel, up to and including dismissal from employment.

The State of New Hampshire and its agencies reserve the right to monitor, to check system performance to ensure computers, systems, and networks are used properly and to restrict activity on the network as appropriate. Individual Authorized Users may not have a personal expectation of privacy for any information they create or receive utilizing State of New Hampshire's IT resources.

The Authorized User shall be cognizant of the fact that the same laws, regulations, and requirements regarding protection, withholding, and disclosure requirements of the *Freedom of Information, Privacy and Federal Records Acts* cover federal government electronic records, including e-mail.

In the event there is a question, each Authorized User shall check with supervisors, management or designees to determine whether particular information is classified as confidential.

Each Supervisor, management or designee is to provide Authorized Users with instruction on maintaining the security of records and the proper release of information in records.

Posting of Policy

This policy, as from time to time amended, shall be publicly posted by the Agency.

AUTHORITY/REFERENCES

RSA 21-G: 9, III

Per 1002.08 (b) (6), (7), (16), (23), (24), (25) and (26)

Department of Information Technology Statewide Standards:
http://www.nh.gov/doit/intranet/toolbox/standards/index.php

EFFECTIVE DATE

This policy is effective as of _____ and shall continue in effect until revoked, amended or superseded.

COMPUTER USE POLICY & AGREEMENT

EMPLOYEE ACKNOWLEDGEMENT

I hereby acknowledge that I have read and understand the foregoing Computer Use Policy and have been given the opportunity to ask any questions that I may have in regard to this Policy. I agree to act in accordance with the Policy, as it may from time to time be amended, and understand that if I do not act in accordance with the Policy, as from time to time amended, I may be subject to disciplinary action as described in the Administrative Rules of the Division of Personnel, up to and including dismissal from employment.

_____	_____
Employee's Signature	Date
_____	_____
Employee's Name in Print	Supervisor Name in Print